



**UNITED STATES PATENT AND TRADEMARK OFFICE**

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/420,877	10/19/1999	ROBERT WESLEY BOSSEMEYER JR.	AIT-0127-PA	3390
7590	11/30/2004		EXAMINER	
ARTZ & ARTZ 28333 TELEGRAPH ROAD SUITE 250 SOUTHFIELD, MI 48034			TRUONG, THANHNGA B	
			ART UNIT	PAPER NUMBER
			2135	

DATE MAILED: 11/30/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	Application No.	Applicant(s)
	09/420,877	BOSSEMEYER ET AL.
	Examiner	Art Unit
	Thanhnga Truong	2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

1) Responsive to communication(s) filed on 10/14/2004 (RCE).  
 2a) This action is **FINAL**.                            2b) This action is non-final.  
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

4) Claim(s) 1-20 is/are pending in the application.  
 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
 5) Claim(s) \_\_\_\_\_ is/are allowed.  
 6) Claim(s) 1-20 is/are rejected.  
 7) Claim(s) \_\_\_\_\_ is/are objected to.  
 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

9) The specification is objected to by the Examiner.  
 10) The drawing(s) filed on 10/19/1999 is/are: a) accepted or b) objected to by the Examiner.  
     Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
     Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
 a) All    b) Some \* c) None of:  
 1. Certified copies of the priority documents have been received.  
 2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

1) Notice of References Cited (PTO-892)  
 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)  
 3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
     Paper No(s)/Mail Date \_\_\_\_\_

4) Interview Summary (PTO-413)  
     Paper No(s)/Mail Date. \_\_\_\_\_

5) Notice of Informal Patent Application (PTO-152)  
 6) Other: \_\_\_\_\_

## DETAILED ACTION

### ***Claim Rejections - 35 USC § 103***

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. Claims 1-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Murphy (US 6,226,744 B1), and further in view of Carper et al (US 6,480,935 B1).

a. Referring to claim 1:

i. Murphy teaches:

(1) a communications network in operative communication with said smart card terminal [i.e., **Figure 1, a smart card 10 is inserted into a smart card reader 12, which is inserted into a 3.5" floppy disk drive of a client terminal, wherein the terminal having a network connection or modem connection to WWW 16 ( column 4, line 33-40)]**; and

(2) a central data base server in operative communication with said communication network [i.e., **client terminal 14 is in communication with a secure gateway server 18, a secure server 22, and an administrative server 24 via WWW 16 (column 4, line 44-46)]**, and

(a) including a plurality of partitioned memory locations [i.e., **Figure 2, main memory 24 may be any type of machine readable storage device, such as RAM, ROM, PROM, and EEPROM (column 5, line 8-13)]**, wherein

(b) at least one of said partitioned memory locations contains information associated with an authorized user of said smart card [i.e., **secure gateway server 18 includes a main memory module, performing read and write information (that is "information associated with an authorized user") to smart card (column 6, line 18-19)]**, whereby

(c) said information being accessible through said smart card terminal via at least one of said memory-economizing data pointers contained within said smart card [**i.e., information from the card is accessed using the program and a PIN, and is compared with server information (column 4, line 23-25)**].

ii. However, Murphy does not explicitly mention:

(1) a plurality of partitioned memory locations; and memory allocation uses memory-economizing data pointers within said smart card.

iii. Carper teaches:

(1) Carper's invention makes full use of a predictable data record format and an efficient file directory structure. While subject to variation and programmer definition, the data record format provides a basis by which the memory management record may be recreated upon smart card initialization by interrogation of the various data object stored in read/write memory. The file directory is flexible and able to accurately identify all data objects persistent in read/write memory, while occupying a minimum of memory space itself, that is similar to "memory-economizing data pointers" (**column 3, lines 9-19**). In addition, memory allocation is made by the memory manager on an "as needed" basis, such that records, files, and data objects are stored in a minimum of memory space. When the OS or an application requires a block of memory, it requests the desired amount from the memory manager. The memory manager identifies and allocates the smallest available block of read/write memory capable of satisfying the request. This process reduces memory space fragmentation and allows optimal use of the memory space. Effective memory management requires a reference. At any given moment, the reference must accurately indicate which portions of memory are in use and which portions are available for allocation. Alternatively, an accounting or a polling algorithm might be used to monitor memory use. A memory management reference can take advantage of the fact that commercial memory devices are often divided into data blocks having a minimum or nominal size (**column 4, lines 32-49**). Furthermore, such macro-partitioning of EPROM between data types, or between individual applications is

common in conventional smart cards. Often, the partitioning creates a fixed memory queue in which one application is written behind the next until the queue is full. Once the queue is full no additional programs may be loaded onto the smart card (**column 2, lines 43-48**).

iv. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) include such smart card memory allocation and deallocation in Murphy's Figure 2, since all requests for smart card memory definition (allocation and deallocation) are controlled by the memory manager, memory integrity and security are assured (**column 2, lines 54-56 of Carper**).

v. The ordinary skilled person would have been motivated to:

(1) include such smart card memory allocation and deallocation in Murphy's Figure 2, since memory allocation may be made dynamically on an as-needed basis, the smart card memory may be efficiently used, and need not be pre-allocated or defined by arbitrary boundaries (**column 2, lines 57-60 of Carper**).

b. Referring to claim 2:

i. Murphy further teaches:

(1) a central time/date authority in operative communication with said communications network [i.e., **Figure 2, an authentication module resides within the secure gateway server which is in communication with network via WWW 16 (column 4, line 44-46 and line 60)**],

(a) said central time/date authority providing a time verification that is associated with said information transmitted between said central database server and said smart card terminal [i.e., **authentication information was stored in database 26 by the same CA (Certified Authority) that issued smart card 10 to user (column 6, line 34-37)**. Any type of user data (that is "a time verification") can be used and still fall within the scope of the invention (**column 14, line 65-66**)].

c. Referring to claims 3-4:

i. Murphy further teaches:

Art Unit: 2135

(1) wherein said communication network is part of a public-switched telephone network; wherein said communication network communicates with said smart card terminal via plain old telephone system (POTS) [i.e., Murphy's invention includes a method and apparatus for authenticating users of a network, such as the Internet or WWW, this clearly involves "public-switched telephone network and plain old telephone system (POTS)". Each network user is assigned a smart card that can be inserted into a smart card reader, that can in turn be inserted into a 3.5" floppy disk drive of a PC. User information is stored on the smart card. Authentication is accomplished by sending messages from the network (e.g., an Internet web site) to the user's PC to interrogate the smart card (column 3, line 66 through column 4, line 7)].

d. Referring to claim 5:

i. Murphy further teaches:

(1) communications network includes the Internet [i.e., **such networks are the Internet (column 1, line 60-61)**].

e. Referring to claim 6:

i. Murphy further teaches:

(1) central database server comprises a network smart card server and a plurality of interconnected database servers [i.e., **Figure 1, servers 18, 20, 22, and 24 (column 4, line 47-48)**].

f. Referring to claim 7:

i. Murphy further teaches:

(1) wherein at least one of said partitioned memory locations includes both a restricted data portion containing information regarding said authorized user accessible to a first predetermined group of network users [i.e., **whenever a user desires to access restricted information stored at various servers protected by secure gateway server 18, the user only has to be authenticated once, then accesses a server having restricted information (column 6, line 58-63)**], and

(2) a public data portion containing information regarding said authorized user that is accessible to a second predetermined group of network

users [i.e., a user was not limited to the information stored on their own computer, but could gain access to information stored on hundreds, even thousands, of individual computers linked together by a single network (column 1, line 57-60)].

g. Referring to claim 8:

i. This claim has limitations that is similar to those of claims 2 and 7, thus it is rejected with the same rationale applied against claims 2 and 7 above.

h. Referring to claim 9:

i. This claim has limitations that is similar to those of claims 1 and 7, thus it is rejected with the same rationale applied against claims 1 and 7 above.

i. Referring to claim 10:

i. Murphy teaches:

(1) providing at least one smart card terminal for receiving and communicatively interacting with said smart card [i.e., **Figure 1, a smart card 10 is inserted into a smart card reader 12, which is inserted into a 3.5" floppy disk drive of a client terminal (column 4, line 33-37)**];

(2) verifying authorization for a desired application that is selected at said smart card terminal for said smart card transaction; transmitting at least an authorization code associated with said smart card both through a communication network and to a network smart card server that includes a plurality of application-specific partitioned memory locations [i.e., **information from the card is accessed using the program and a PIN or an access code, and is compared with server information (column 4, line 23-25)**. In addition, the specific data being stored and retrieved from the smart card in this example of a smart card interface module is in the form a user's social security number (SSN) for use in authenticating the user. It can be appreciated, however, that any type of data could be stored or retrieved from the smart card, such as tickets, certificates, public/private keys, and so forth. (column 7, line 22-28)];

(3) utilizing at least one data pointer provided by said authorization code to point to information relating to said authorized user that is contained in at least one of said application-specific partitioned memory location [i.e.,

Art Unit: 2135

**authentication information (that is "information relating to said authorized user") was stored in database 26 by the same CA (Certified Authority), such as tokens, digital signatures, certificates, etc., that issued smart card 10 to user ( column 5, line 54-57 and column 6, line 34-37)]; and**

**(4) transmitting said information through said communications network to said smart card terminal [i.e., authentication module 32 uses the smart card interface module and the PIN to access and read/write user information from/to smart card 10 via WWW 16 (column 6, line 29-32)].**

ii. However, Murphy does not explicitly mention:

(1) a plurality of application-specific partitioned memory locations within said smart card.

iii. Carper teaches:

(1) memory allocation is made by the memory manager on an "as needed" basis, such that records, files, and data objects are stored in a minimum of memory space. When the OS or an application requires a block of memory, it requests the desired amount from the memory manager. The memory manager identifies and allocates the smallest available block of read/write memory capable of satisfying the request. This process reduces memory space fragmentation and allows optimal use of the memory space. Effective memory management requires a reference. At any given moment, the reference must accurately indicate which portions of memory are in use and which portions are available for allocation. Alternatively, an accounting or a polling algorithm might be used to monitor memory use. A memory management reference can take advantage of the fact that commercial memory devices are often divided into data blocks having a minimum or nominal size (**column 4, lines 32-49; for further details of how memory is being partitioned, see Figures 3-5 and column 6, line 10 through column 9, line 13**). Furthermore, such macro-partitioning of EPROM between data types, or between individual applications is common in conventional smart cards. Often, the partitioning creates a fixed memory queue in which one application is written behind the next until the queue is full. Once the queue

is full no additional programs may be loaded onto the smart card (**column 2, lines 43-48**).

iv. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) include such smart card memory allocation and deallocation in Murphy's Figure 2, since all requests for smart card memory definition (allocation and deallocation) are controlled by the memory manager, memory integrity and security are assured (**column 2, lines 54-56 of Carper**).

v. The ordinary skilled person would have been motivated to:

(1) include such smart card memory allocation and deallocation in Murphy's Figure 2, since memory allocation may be made dynamically on an as-needed basis, the smart card memory may be efficiently used, and need not be pre-allocated or defined by arbitrary boundaries (**column 2, lines 57-60 of Carper**).

j. Referring to claim 11:

i. Murphy further teaches:

(1) modifying said information as accessed at said smart card terminal; transmitting said information as modified to said network smart card server; and storing said information as modified in at least one of said application-specific partitioned memory locations [**i.e., this claim has some limitations that is similar to those of claim 1, thus it is rejected with the same rationale applied against claim 1 above. In addition, Figure 1, a situation may arise where a user may want to access/change user information on smart card, the administrative module allows a user to verify and change a PIN. Any user modifications made at administrative server 24 are replicated to user's authentication profile stored in database 26 (column 7, line 5-10)**].

k. Referring to claim 12:

i. This claim has limitations that is similar to those of claim 2, thus it is rejected with the same rationale applied against claim 2 above.

l. Referring to claim 13:

Art Unit: 2135

i. This claim has limitations that is similar to those of claim 11, thus it is rejected with the same rationale applied against claim 11 above.

m. Referring to claim 14:

i. Murphy teaches:

(1) a microprocessor programmed to received an authorization code associated with said smart card, said authorization code representing a data pointer for pointing to authorized user related information contained within at least one memory location within said first or second plurality of partitioned memory locations [i.e., **this claim has some limitations that is similar to those of claim 1, thus it is rejected with the same rationale applied against claim 1 above.** In addition, Figure 2, the overall functioning of secure gateway server is controlled by a central processing unit (CPU) 26, which operates under the control of executed computer program instructions that are stored in main memory (column 4, line 66-67 and column 5, line 1-2). Bus adapter 30 is used for transferring data back and forth between CPU/memory bus and I/O bus (column 5, line 37-38)].

n. Referring to claim 15:

i. Murphy further teaches:

(1) wherein said information contained in first plurality of application-specific partitioned memory locations is access-designated public data for said smart card transactions [i.e., **this claim has some limitations that is similar to those of claims 1 and 14, thus it is rejected with the same rationale applied against claims 1 and 14 above.** In addition, a user was not limited to the information stored on their own computer, but could gain access to information stored on hundreds, even thousands, of individual computers linked together by a single network (column 1, line 57-60)].

o. Referring to claims 16:

i. This claim has limitations that is similar to those of claim 15, thus it is rejected with the same rationale applied against claim 15 above.

p. Referring to claim 17:

i. This claim has limitations that is similar to those of claim 1, thus it is rejected with the same rationale applied against claim 1 above.

q. Referring to claim 18:

i. Murphy further teaches:

(1) one of said first plurality of application-specific partitioned memory locations is located on a separate database server accessible through a communication network [i.e., **this claim has some limitations that is similar to those of claims 1 and 14, thus it is rejected with the same rationale applied against claims 1 and 14 above. In addition, Figure 1, Secure gateway server 18 is in communication with WWW 16, whereas database 26 could be stored on server 18 as well (column 4, line 54)**].

r. Referring to claims 19-20:

i. These claims have limitations that is similar to those of claims 3-4, thus they are rejected with the same rationale applied against claims 3-4 above.

### **Conclusion**

3. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. De Jong et al (US 6,769,053 B1) discloses computer-readable medium storing a data structure for supporting persistant storage of a set of data, the data structure including: (a) at least an oldest version of the set of data in first memory area, the first memory area including at least one first tag for uniquely identifying the oldest version, and (b) at least a most recently updated version of the set of data in a second, distinct memory area, the second memory area including at least one second tag for uniquely identifying the most recently updated version (see abstract).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 571-272-3858.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached at 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

TBT

November 23, 2004



KIM VU  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100